編 者 的 話

量子電腦能同時處理 2^n 個量子態, 因此在某些問題上遠比傳統電腦高效。現有公開金鑰系統可被 Shor 演算法在多項式時間內破解。後量子密碼學 (Post-Quantum Cryptography, PQC) 致力於建立能夠抵抗量子電腦攻擊的公鑰密碼系統。周彤教授介紹後量子密碼學的最新發展, 說明量子電腦對現有密碼系統的威脅、NIST 的標準化進程, 以及他在後量子密碼學領域的研究成果。他指出未來值得投入的方向: 橢圓曲線同源密碼學、「腦內多方計算」簽章, 以及代數攻擊。

看似簡單的組合填表問題, 背後蘊含深刻的代數與幾何結構。劉士瑋博士以「在方格中填入遞增數字的組合問題」爲起點, 逐步引入 Catalan 數、鉤長公式、對稱函數、Schur 函數、Kostka 數、Macdonald 常數項公式, 闡述一條從初等組合到現代代數的知識鏈。

數學與詩在思維方式、結構追求與直觀本質上具有深刻共通性。爲何許多數學家喜歡詩、甚至寫詩? 何崇武教授以自身經驗與廣泛例證提出說明, 首先是結構感的共鳴: 詩的格律與數學的邏輯架構相似; 數學家因習慣尋找「結構」, 因此更能欣賞詩的形式之美。其次是直觀的共同性: 兩者皆依賴深層直覺與類比; 文末引用物理學家 Peterson 的研究, 指出但丁《神曲》中的宇宙模型竟與廣義相對論的封閉宇宙相吻合, 反映詩人與科學家在「深層直觀」上可能相通。第三是語言的精煉: 詩與數學都追求最簡潔的表達方式。第四是情感與理性的互補: 詩補足數學無法觸及的價值、目的與情感層面。

何教授在文末介紹了超現實數 (surreal number) 及劉維爾數 (Liouville number)。John Conway 以遞迴方式從空集合構造出超現實數, 這是一個包括實數、無窮小量、超限序數的龐大有序域。其構造方法本身極具美感, 並與博弈論相關。劉維爾數是一類能被有理數「極佳近似」的超越數。Liouville 以階乘分母的小數展開構造出的超越數, 其數量不可數。這些數在數軸上測度爲零, 但結構極爲豐富。

冼鏡光探討《幾何原本》中與畢氏定理相關的四個命辭, 包括畢氏定理本身、餘弦定律的幾何版本、以相似三角形分割直角三角形, 以及相似多邊形版本的畢氏定理。冼教授說明這四個命辭如何構成一個完整的幾何體系, 爲畢氏定理與餘弦定律提供幾何基礎。他同時回顧了歷史上不同證明方法的演變。

冼教授提出「歐基里德剪刀」這個現代名稱, 指的是在三角形每個頂點構造兩個面積相等的三角形 (由邊與正方形邊組成)。他進一步解釋,「剪刀算法」可用來證明畢氏定理及餘弦定律, 而早在 17 世紀, 耶穌會學者已使用剪刀法證明了餘弦定律。

數學傳播電子版網址:

https://www.math.sinica.edu.tw/mathmedia

梁惠禎
2026 年 3 月

數學傳播 197 第五十卷 第一期

目錄

淺談後量子密碼學近期發展 ······················ 周　彤　3

對稱函數在組合問題中的應用 ······················ 劉士瑋　6

數學與詩 ······························ 何崇武　11

畢氏定理的三角學證明: II

畢氏定理:《幾何原本》中究竟證明了什麼? · 冼鏡光　26

輪環多面體框正多面體的屬性數及其建構

在數學算板上的實踐 ······················ 林保平　43

從 $\sqrt{2}$ 談起 — 謹以此文紀念元老 (1930~2021) · 林開亮　55

利用兩相鄰完全平方數來證明恆等式

$[\sqrt{9n+8}]=[\sqrt{n}+\sqrt{n+1}+\sqrt{n+2}]$ ······· 李維昌　68

對數播 173 期張進安老師一文的回響 ·············· 連威翔　76

以三角形圖形組建 $\cos\left(\frac{\pi}{7}\right)$ 的相關方程式並求解其函數值

表示式 ······························ 李輝濱　86

本原 Heron 數組公式及若干相關結果 ············ 吳　波　117

由畢氏定理的一種證明發現的結論 ················ 甘志國　139

應用極座標法證明蘭勃特定理 ···················· 于志洪　145

千姿百態的玫瑰線 ························ 薛黨鵬　148